

U.S. Serial No. 09/940,982

NIT-295

IN THE CLAIMS

1. (Currently amended) An information-processing apparatus serving as a data-processing means for carrying out predetermined processing OP1 on input data D1 in order to produce a result of said predetermined processing as processed data D2, said information-processing apparatus comprising:

a data transform means for transforming said input data D1 by using disturbance data XI to generate transformed data H1;

a transformed-data-processing means for carrying out said predetermined processing OP1 for said input data D1 or processing different from said predetermined processing OP1 to replace said predetermined processing OP1 on said transformed data H1 in order to generate processed transformed data H2; and

a data inverse-transform means for carrying out inverse-transformation processing OP2 on said processed transformed data H2 by using processed disturbance data XO in order to generate said processed D2 which can also be obtained without transformations as a result of said predetermined processing OP1 carried out on said input data D1,

wherein said disturbance data XI and said processed disturbance data XO each have ~~a constant or all but constant~~

U.S. Serial No. 09/940,982

NIT-295

~~hamming weight~~ a constant hamming weight.

2. (Currently amended) An information-processing apparatus according to claim 1, wherein said processed disturbance data XO is generated by carrying out said predetermined processing OP1 on said disturbance data XI.

3. (Currently amended) An information-processing apparatus according to claim 1, wherein each bit of said processed disturbance data XO and said disturbance data XI has a logic value of 0 or 1 at a probability of 50%.

4. (Currently amended) An information-processing apparatus according to claim 1, said information-processing apparatus further having a disturbance-data and processed-disturbance-data generation means capable of generating said disturbance data XI having a constant ~~or all but constant~~ hamming weight and generating said processed disturbance data XO having a constant ~~or all but constant~~ hamming weight by execution of input-data processing defined in advance on said disturbance data XI.

U.S. Serial No. 09/940,982

NIT-295

5. (Currently amended) An information-processing apparatus according to claim 1, said information-processing apparatus further having:

a disturbance-data storage means for storing a plurality of candidates for said disturbance data XI having ~~uniform or all but uniform hamming weights~~ uniform hamming weights; and

a disturbance-data select means for randomly selecting one of said candidates for said disturbance data XI stored in said disturbance-data storage means,

wherein disturbance-data processing is carried out to process said selected candidate for said disturbance data XI in order to generate said processed disturbance data XO.

6. (Original) An information-processing apparatus according to claim 1, said information-processing apparatus further having a constant-hamming-weight-random-number generation means used for generating random numbers with uniform constant hamming weights and provided with:

a random-number generation means for generating random numbers each having a hamming weight equal to half the number of bits included in said generated random number;

a bit inversion means for inverting bits of data; and

a bit concatenation means for concatenating a random

U.S. Serial No. 09/940,982

NIT-295

number generated by said random-number generation means with data output by said bit inversion means as a result of inversion of said random number generated by said random-number generation means.

7. (Original) An information-processing apparatus according to claim 1, said information-processing apparatus further having:

a random-number generation means for generating a random number to be used as said disturbance data XI;

a hamming-weight computation means for computing a hamming weight of a random number generated by said random-number generation means;

a hamming-weight examination means for examining said hamming weight computed by said hamming-weight computation means; and

a constant-hamming-weight assurance means for requesting said random-number generation means to generate another random number for said hamming-weight examination means' result of examination indicating an inspected hamming weight not equal to a target hamming weight.

U.S. Serial No. 09/940,982

NYT-295

8. (Original) An information-processing apparatus according to claim 1, said information-processing apparatus further having a constant-hamming-weight-random-number generation means used for generating random numbers with uniform constant hamming weights and provided with:

a constant-hamming-weight and constant-fractional-bit-count random-number generation means used for generating partial random numbers with uniform constant hamming weights and uniform bit counts each equal to a fraction of the bit count of a final random number to be generated;

a random-number-generation control means for controlling said constant-hamming-weight and constant-fractional-bit-count random-number generation means to generate partial random numbers till a sum of bit counts of said partial numbers equal to said bit count of said final random number; and

a data concatenation means for concatenating said partial random numbers generated by said constant-hamming-weight and constant-fractional-bit-count random-number generation means to result in said final random number.

9-17. (Canceled).